REMARKS

Claims 1-30 are currently pending. In the Office Action dated September 5, 2007, claim 27 was rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Claims 1, 2, 4-9, 11, 13-17, 19, 21-25, and 27-29 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,918,113 to Patel ("Patel"). Claims 3, 10, 12, 18, 20, 26, and 30 were rejected under 35 U.S.C. §103(a) as being unpatentable over Patel in view of U.S. Patent No. 6,810,525 to Safadi ("Safadi"). By this amendment claims 1-10 and 27-30 have been canceled without prejudice or disclaimer rendering their rejections moot.

Interview Summary

On September 20, 2007, Applicants' attorney conducted a telephone interview with the Examiner. Applicants' attorney pointed out that Patel was incorrectly characterized as performing certain functions on the client system, whereas Patel actually performed the functions on the License and Application Servers. Applicants further requested that the finality of the most recent Office Action be withdrawn in view of Patel failing to show all the claim limitations.

Discussion of the Disclosed Embodiments

The disclosed embodiments of the invention will now be discussed in comparison to the prior art. Of course, the discussion of the disclosed embodiments, and the discussion of the differences between the disclosed embodiments and the prior art subject matter, do not define the scope or interpretation of any of the claims. Instead, such discussed differences merely help the Examiner appreciate important claim distinctions discussed thereafter.

Applicants disclose, in one embodiment, a method for allowing a user at a remote computer system to access a computer resource, such as an application. A token is generated remote from the computer system, such as at a server, and is then transmitted to the user's computer system, such as by means of a smart card storing the token. The token contains encrypted user information including credit, authorization, and authentication information. The computer resource may be independently usable on the user's client system or may be a module allowing remote access to an application or other resource stored on a server. The computer

resource is encrypted such that the user may access it only upon completion of authorization and verification steps discussed below.

A request is initiated to open the encrypted computer resource stored on the computer system, and execution of a remote application manager component on the client system is also initiated. Under the control of the remote application manager component, the token is decrypted at the client system and a user is authenticated on the client system using authentication information stored in the token. Whether the user is authorized to use the requested computer resource is determined on the client system by the remote application manager component using authorization information stored in the token. The remote application manager component also verifies whether the user has sufficient credit contained in the token to use the requested computer resource using credit information stored in the token. When the user is authenticated, authorized, and has sufficient credit, the requested computer resource is decrypted on the client system and opened. Use of the computer resource is then monitored on the client system to determine whether the user has sufficient credit to continue using the computer resource. A notification is provided when the monitored usage of the opened computer resource has exceeded the credit.

The disclosed embodiment provides the distinct advantage that it is usable in both continuous- and broken-connection modes of operations. That is to say that, the token may be used to verify and authenticate on the client system in instances where an application executes on the user's client system and where the user interacts with an application executing on a remote server. It further does not require server resources as in the references cited by the Examiner.

Discussion of the Cited References

The system disclosed by Patel is substantially different from the embodiments disclosed by Applicants. In the system of Patel, authentication and verification of a token occur on a server rather than on a client computer system.

Patel discloses an application serving system in which a client system obtains an encrypted access token for a streamed application from a license server. Col. 2, lns. 50-52. The client system sends the encrypted access token to the server. Figure 22 ("Client sends token and Application file page identifiers"); Col. 9, lns. 9-28 ("Once the client obtains an 'Access token'

to run an application, it connects to the application Server 107 and *presents to it the 'Access token'* along with the request for the application bits." (emphasis added)).

The application server then validates the token to determine whether a client can access the streamed application. Figure 22 ("validate token" in box 2210); Col. 26, ln. 65 – Col. 27, ln. 13. ("*The Application Server 2210 needs only to decrypt the Access Token* (or a digest of it) via a secret key shared 2209 with the License Server 2205 (thus verifying the Token is valid), then checking the validity of its contents, e.g., application identifier, and testing the expiration time." (emphasis added)).

Patel does *not* perform any token validation or decryption based on a token at a client system. Patel specifically states that "the 'Access token' is opaque to the client 113 since it does not have the key to decrypt it. The Application Server 107 validates the 'Access token' by decrypting it using a 'decryption key' obtained from the Server Config Database...." Col. 9, lns. 13-18 (emphasis added).

Patel further does not decrypt a computer resource at the client system using the token as in Applicants' disclosed embodiments. Patel teaches only that the token is used to unlock a resource at the server. "*The Application Server 107 validates the 'Access token'* by decrypting it using a 'decryption key' obtained from the Server Config Database 103 and checking the content against a predefined value like for example the Application ID and also by making sure that the expiration time in the 'Access token' has not elapsed. It then serves the appropriate bits to the client 113 to enable it to run the application." Col. 9, lns. 15-23. (emphasis added).

Patel further does not monitor usage at the client system to make sure that a client has not exceeded a usage time limit. Patel instead performs this function at the server. Col. 9, lns. 15-23. (The Application Server 107 validates the 'Access token' by ... checking the content against a predefined value like for example the Application ID and also by *making sure that the expiration time in the 'Access token' has not elapsed*." (emphasis added)).

Safadi fails to remedy the deficiencies of Patel.

Discussion of the Claims

Turning now to the claims, the differences between the cited references and the claimed invention will be particularly pointed out.

With respect to claim 11, the cited references fail to teach a method including the steps of:

under control of a client system,

providing user information to a server system, the user information including authentication, authorization, and credit information for a user of the client system;

receiving from the server system, a token including encrypted information generated from the user information provided by the client system;

a remote application manager component; and

at least one computer resource, each computer resource being encrypted and the particular computer resources received being determined from the authorization information contained in the provided user information;

under control of the remote application manager component on the client system,

decrypting ***at the client system*** *the token in response to a request to initiate execution of one of the computer resources;*

authenticating the user of the client computer system;

verifying whether the user is authorized to use the requested computer resource;

verifying whether the user has sufficient credit contained in the token to use the requested computer resource;

when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the requested computer resource; and

monitoring the usage of the executing computer resource and providing a notification when the monitored usage has exceeded the user's credit.

With respect to claim 19, the cited references fail to teach or suggest a method including the steps of:

under control of a client system,

providing user information to a server system, the user information including authentication, authorization, and credit information for a user of the client system;

under control of a server system,

generating a token including encrypted information generated from the user information provided by the client system;

sending the token to the client system;

sending a remote application manager component to the client system;

sending at least one computer resource to the client system, each computer resource that is sent being encrypted;

under control of the remote application manager component on the client system,

initiating execution of the remote application manager component in response to a request to initiate execution of the computer resource;

decrypting ***at the client system*** *the token and authenticating a user of the client computer system;*

verifying ***at the client system*** *whether the user is authorized to use the computer resource;*

verifying ***at the client system*** *whether the user has sufficient credit contained in the token to use the computer resource;*

when the user is authenticated, authorized, and has sufficient credit, decrypting and initiating execution of the computer resource; and

monitoring the usage of the executing computer resource ***at the client system*** *and providing notification when the monitored usage has exceeded the user's credit.*

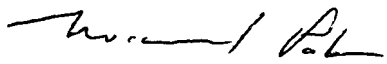
Claims 12-18 and 20-26 are dependent on claims 11 and 19 respectively and are therefore allowable.

Conclusion

Applicants note that the failure of Patel to teach or suggest all of the claim limitations of claims 11 and 19 was pointed out in the prior-filed Office Action response. Applicants therefore request that the claims be allowed or that the finality of the most recent Office Action be withdrawn if additional search finds more relevant prior-art references.

Respectfully submitted,

DORSEY & WHITNEY LLP



Michael G. Pate
Registration No. 53,439
Telephone No. (206) 903-2398

MGP:sp

Enclosures:
Postcard
Fee Transmittal Sheet (+ copy)

DORSEY & WHITNEY LLP
1420 Fifth Avenue, Suite 3400
Seattle, WA 98101-4010
(206) 903-8800 (telephone)
(206) 903-8820 (fax)

h:\ip\clients\micron technology\700\500767.01\500767.01 amend af 090507.doc